LÖSUNGSHINWEIS

LOOKALIKE-DOMAIN-ÜBERWACHUNG SCHÜTZT IHR NETZWERK, IHRE KUNDEN UND IHRE MARKE

Stoppen Sie proaktiv Social-Engineering-Bedrohungen durch den Einsatz von Lookalike-Domains in fortschrittlichen gezielten Angriffen, die darauf abzielen, das Unternehmen zu kompromittieren, Kunden zu gefährden oder Ihre wertvolle Marke zu schädigen.

EINE WACHSENDE BEDROHUNG DURCH LOOKALIKES

Von großvolumigen, breit gefächerten Angriffen auf Verbraucherebene bis hin zu hochgradig zielgerichtetem Spear-Phishing, Business Email Compromise (BEC) und anderen Bedrohungen für Unternehmen sind Lookalike-Domains zu Schlüsselkomponenten geworden, die Angreifern helfen, sowohl menschliche als auch technische Abwehrmechanismen zu umgehen. Sie können sich als Ihre Marke, Ihre Mitarbeiter, Ihre Lieferkette oder andere vertrauenswürdige Partner ausgeben – mit verheerenden Folgen.

Obwohl sie schon vor fast zwei Jahrzehnten erstmals eingesetzt wurden, entwickeln Bedrohungsakteure weiterhin neue Methoden, um ähnlich aussehende Domains in neuen Angriffstypen zu verwenden. Mithilfe von Adversary-in-the-Middle (AitM)-Techniken versuchen sie immer häufiger, den Mitarbeitern vorzugaukeln, dass sie während der Authentifizierung mit dem echten Netzwerk des Unternehmens interagieren.

Heutzutage verwenden Angreifer ähnlich aussehende Domains in SMS-Nachrichten, Telefonanrufen, Direktnachrichten in sozialen Medien, E-Mails und QR-Codes. In jüngster Zeit haben Angreifer die Multi-Faktor-Authentifizierung (MFA) ins Visier genommen, da diese von Spielern bis hin zu Marktplätzen, Wallets und Börsen für digitale Währungen immer häufiger genutzt wird, wie z. B. bei dem Angriff auf Coinbase Anfang 2023. Lookalikes sind zu einem festen Bestandteil jeder größeren Cyber-Bedrohung geworden.

EINE WACHSENDE BEDROHUNG DURCH LOOKALIKES

Abbildung 1: Infoblox Threat Intelligence hat überraschende Forschungsdaten über das zunehmende Risiko von Lookalike-Domains geteilt.

ZAHLEN UND FAKTEN

Andere erweiterte Sicherheitsfunktionen von BloxOne Threat Defense ermöglichen es Ihnen:

- In etwas mehr als einem Jahr wurden über 300 000 Lookalike-Domains entdeckt
- Combosquatting-Domains sind jetzt 100-mal häufiger als Typosquatting
- Jeden Tag werden 200.000 neue Domains erstellt
- Mehr als 1.600 Domains wurden im Jahr 2023 verwendet, um offizielle MFA-Dienste zu imitieren
- 60 % der Combosquatting-Domains sind seit über 1.000 Tagen aktiv
- Abgesehen von der Nutzung von .com gibt es heute 1.588 andere TLDs für den Missbrauch durch Angreifer.
- DNS wird bei 92 % der Cyberangriffe verwendet.

SCHUTZ IHRER MARKE UND IHRER KUNDEN

Die Abwehr von Bedrohungen durch Lookalike-Domains für Unternehmen erfordert einen anderen Ansatz als der, der bei eher verbraucherorientierten, massenmarktorientierten Angriffen verwendet wird. Mit Infoblox Lookalike Domain Monitoring verwalten die Kunden ihre eigene Liste der Domains, von denen sie befürchten, dass sie gegen sie, ihre Mitarbeiter oder ihre Kunden verwendet werden könnten. Infoblox Threat Intelligence überwacht dann globale Registrare, ISPs, die tatsächliche DNS-Aktivität und mehr, um potenzielle hochriskante Lookalike-Domains anhand der Überwachungsliste des Kunden zu identifizieren und mit der ersten Bewertung und Überwachung zu beginnen. Die Lookalike-Domain-Monitoring-Schnittstelle bietet den Kunden Einblick in identifizierte Lookalikes mit hohem Risiko und Risikoprofildaten, die dem Unternehmen helfen, fundierte Entscheidungen zu treffen, um proaktiv eine potenzielle Netzwerkverletzung, eine Gefährdung der Kunden oder eine Schädigung des Rufs und der Marke des Unternehmens zu verhindern.

Das Lookalike Domain Monitoring ist separat erhältlich und im Abonnement der branchenführenden DNS-Erkennungs- und -Antwortlösung (DNSDR) BloxOne Threat Defense Advanced von Infoblox enthalten. Diese Lösungen erlauben es Kunden, einen ersten Satz benutzerdefinierter Domains zu identifizieren, die auf risikoreiche Lookalikes überwacht werden sollen. Kunden, die mehr Domains auf diese Risiken überwachen lassen möchten, können zusätzliche Lizenzen in Schritten von 100 Domains erwerben.

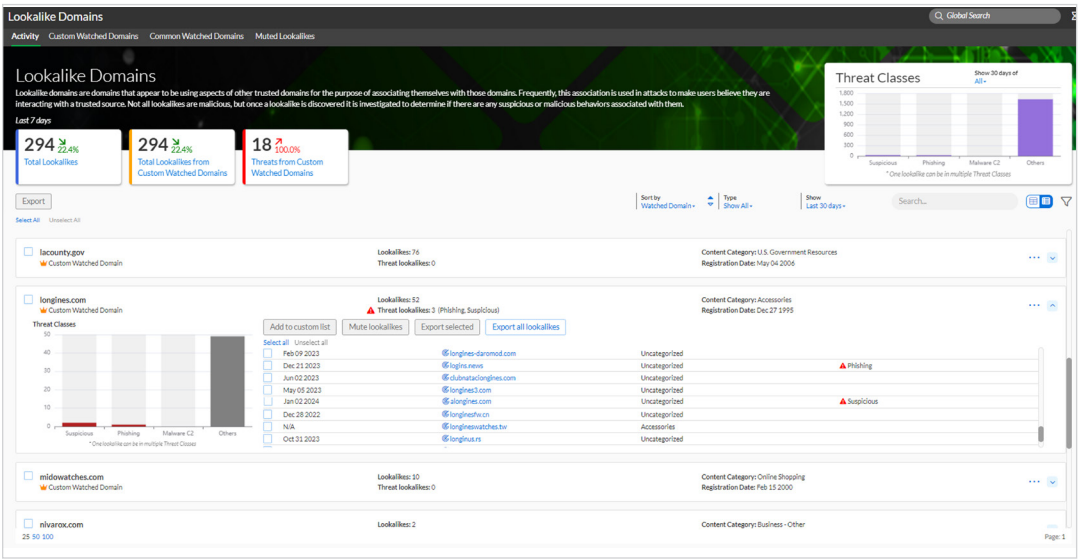

Abbildung 2: Überprüfen Sie einfach hochriskante Lookalike-Domains, um die von ihnen ausgehenden Risikostufen zu verstehen

INTERNETBETRUG DURCH DEN MISSBRAUCH VON LOOKALIKES STOPPEN

Infoblox bietet „Domain Mitigation Services“ an, um Kunden dabei zu helfen, Domains, die ein Risiko für ihre Unternehmen oder Kunden darstellen, schnell zu entfernen. Wir wenden die proprietäre Mischung aus investigativen Fähigkeiten, automatisierten Techniken und Branchenbeziehungen von Infoblox an, um Probleme mit branchenführenden SLAs zu lösen, die in Stunden gemessen werden, einschließlich Datendiebstahl, Website-Spoofing und anderer Cybervorfälle, schnell und diskret.

Weitere Informationen zu Infoblox Domain Mitigation Services finden Sie unter https://insights.infoblox.com/de-resources/der/infoblox-datasheet-infoblox-domain-mitigation-services-de

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com/de

Version: 20240125v3